Qubit-based Unclonable Encryption with Key Recycling

Daan Leermakers, Boris Škorić

Abstract

We re-visit Unclonable Encryption as introduced by Gottesman in 2003 [9]. We look at the combination of Unclonable Encryption and Key Recycling, while aiming for low communication complexity and high rate.
We introduce a qubit-based prepare-and-measure Unclonable Encryption scheme with re-usable keys. Our scheme consists of a single transmission by Alice and a single classical feedback bit from Bob. The transmission from Alice to Bob consists entirely of qubits. The rate, defined as the message length divided by the number of qubits, is higher than what can be achieved using Gottesman's scheme [9]. We provide a security proof based on the diamond norm distance, taking noise into account.

1 Introduction

1.1 Doing better than One-Time Pad encryption

Classically, the best confidentiality guarantee is provided by One-Time Pad (OTP) encryption. If Alice and Bob share a uniform n-bit secret key, they can exchange an n-bit message with information-theoretic security. In the classical setting Eve is able to save a copy of the ciphertext. For the message to remain secure in the future, two conditions must be met:

1. The key is used only once.

2. The key is never revealed.

If a quantum channel is available, these conditions can both be relaxed. (i) Quantum Key Recycling (QKR) [5,12,15] schemes provide a way of re-using encryption keys. (ii) Unclonable Encryption (UE) [9] guarantees that a message remains secure even if the keys leak at some time in the future.
In this paper we introduce a sheme that achieve both the key recycling and UE properties, and we explicitly prove that this can be achieved with low communication complexity. Our scheme acts only on individual qubits with simple prepare-and-measure operations.

1.2 Quantum Key Recycling

The most famous use of a quantum channel in the context of cryptography is Quantum Key Distribution (QKD). First proposed in 1984 [4], QKD allows Alice and Bob to extend a small key, used for authentication, to a longer key in an information-theoretically secure way. Combined with classical OTP encryption this lets Alice and Bob exchange messages with theoretically unconditional security. The QKD field has received a large amount of attention, resulting in QKD schemes that discard fewer qubits, various advanced proof techniques, improved noise tolerance, improved rates, use of EPR pairs, higher-dimensional quantum systems etc. [1,2,8,10,13,16,19–22]. Much less known is that the concept of QKR was proposed

two years before QKD [5]. QKR allows for the re-use of the secret encoding key when no disturbance is detected. QKD and QKR have a lot in common. (i) They both encode classical data in quantum states, in a basis that is not a priori known to Eve. (ii) They rely on the no-cloning theorem [25] to guarantee that without disturbing the quantum state, Eve can not gain information about the classical payload or about the basis.

The security of QKD has been well understood for a long time [e.g. 8, 19–21], while a security proof for qubit-based QKR has been provided fairly recently [12]. A cipher with near optimal rate using high-dimensional qudits was introduced in 2005 [7]. Unfortunately, their method requires a quantum computer to perform encryption and decryption. In 2017, a way of doing authentication (and encryption) of quantum states with Key Recycling was proposed [18]. However this work did not lead to a prepare-and-measure variant.

The main advantage of QKR over QKD+OTP is reduced round complexity: QKR needs only two rounds. After the communication from Alice to Bob, only a single bit of authenticated information needs to be sent back from Bob to Alice. Recently, it was shown that QKR over a noisy quantum channel can achieve the same communication rate as QKD (in terms of message bits per qubit) even if Alice sends only qubits [14]; a further reduction of the total amount of communicated data.

1.3 Unclonable Encryption

In 2003, D. Gottesman introduced a scheme called *Unclonable Encryption*[1] (UE) [9] where the message remains secure even if the encryption keys leak at a later time (provided that no disturbance is detected). His work was motivated by the fact that on the one hand many protocols require keys to be deleted, but on the other hand permanent deletion of data from nonvolatile memory is a nontrivial task. In this light it is prudent to assume that all key material which is not *immediately* discarded is in danger of becoming public in the future; hence the UE security notion demands that the message stays safe even if all this key material is made public after Alice and Bob decide that they detected no disturbance. (In case disturbance is detected, the keys have to remain secret forever or permanently destroyed.)

Gottesman remarked on the close relationship between UE and QKD, and in fact constructed a QKD variant from UE. The revealing of the basis choices in QKD is equivalent to revealing keys in UE. It is interesting to note that Gottesman's UE construction allows partial re-use of keys. However, it still expends one bit of key material per qubit sent. In the current paper we introduce qubit-based UE without key expenditure.

Since QKR sends a message directly instead of establishing a key for later use, QKR protocols are natural candidates to have the UE property. In the case of noiseless quantum channels, the high-dimensional encryption scheme [7] and the qubit-based schemes [12, 15] seem to have UE; for noisy channels [15] with modified parameters also seems to have UE. However, none of these conjectures have been explicitly stated or proven, which is a shame since resilience against key leakage is an interesting security feature. The QKR protocol where Alice sends only qubits [14] is clearly not unclonable, due to the fact that single-use keys are stored at the end of each round.

---

[1]This is slightly different from the unclonability notion of Broadbent and Lord [3] which considers two collaborating parties who both wish to recover the plaintext.

2 Contributions

We investigate the possibility of constructing an Unclonable Encryption scheme with recyclable keys, while aiming for low communication complexity and high rate.
We consider the following setting. Alice and Bob have a reservoir of shared key material. Alice sends data to Bob in N chunks. Each chunk individually is tested by Bob for consistency (sufficiently low noise and valid MAC). In case of `reject` they have to access new key material from the reservoir. In case of `accept`, Alice and Bob re-use their key material; this may be done either by keeping keys unchanged or by re-computing keys without accessing the reservoir. If the N'th round was an `accept`, all keys of round N are assumed to become public.

- We define the Key Recycling (KR) and Unclonable Encryption (UE) properties in terms of the diamond norm. For this definition we show a relation between KR and UE: If a KR scheme re-uses all its long-term secrets in unchanged form upon `accept`, then it also has the UE property.

- We introduce `KRUE`, a qubit-based prepare-and-measure scheme that satisfies KR and UE. (Upon `accept` some of the keys are kept and some are updated.) Alice sends a single transmission, which consists entirely of qubits. Bob responds with a single classical feedback bit. We provide a security proof by upper bounding the diamond distance between the protocol and its idealized functionality. In particular, we use a reduction to the diamond distance that is associated with the security of QKD [19]. In the case of a noiseless channel this reduction is almost immediate, without involving any inequalities. For a noisy quantum channel `KRUE`'s asymptotic communication rate equals the asymptotic QKD rate minus $h(\beta)$, where β is the bit error rate of the quantum channel and h is the binary entropy function. The difference in rate is caused by the fact that part of the message in `KRUE` is a new mask for protecting a syndrome in the next round.

- Next we introduce `KRUE`*, a stripped down version of `KRUE` which needs an external mechanism for transporting the next-round mask. For the external mechanism we propose a QKR scheme [14]. This has the advantage that Alice still needs only a single transmission which consists entirely of qubits. The rate of the combined scheme QKR+`KRUE`* is higher than the rate of `KRUE` but lower than the QKD rate. Also, if one would combine Gottesman's scheme with a secure key update mechanism in order to get the KR property, the rate of that combination would be half the rate of QKR+`KRUE`*.

The outline of the paper is as follows. After introducing notation and preliminaries in Section 3, we introduce the attacker model and security definition in Section 4. We then introduce the `KRUE` protocol (Section 5) and provide its security proof (Section 6). In Section 7 we introduce `KRUE`* and discuss its composition with QKD and QKR as external mechanisms to transport the new mask. Finally, in Section 8 we compare our schemes to existing qubit-based alternatives.

3 Preliminaries

3.1 Notation and terminology

Classical Random Variables are denoted with capital letters, and their realisations with lowercase letters. The expectation with respect to X is denoted as $\mathbb{E}_x f(x) = \sum_{x \in \mathcal{X}} \Pr[X = x] f(x)$.

For the ℓ most significant bits of the string s we write $s[:\ell]$. The Hamming weight of a string s is denoted as $|s|$. The notation 'log' stands for the logarithm with base 2. The notation h stands for the binary entropy function $h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$. Sometimes we write $h(p_1, \ldots, p_k)$ meaning $\sum_{i=1}^{k} p_i \log \frac{1}{p_i}$. Bitwise XOR of binary strings is written as '$\oplus$'. The Kronecker delta is denoted as δ_{ab}. We will speak about 'the bit error rate β of a quantum channel'. This is defined as the probability that a classical bit x, sent by Alice embedded in a qubit, arrives at Bob's side as the flipped value $\bar{x}$. A linear error-correcting code with a $\ell \times n$ generator matrix G can always be written in systematic form, $G = (\mathbb{1}_\ell | \Gamma)$, where the $\ell \times (n - \ell)$ matrix Γ contains the checksum relations. For message $p \in \{0,1\}^\ell$, the codeword $c_p = p \cdot G$ then has p as its first ℓ bits, followed by $n - \ell$ redundancy bits.

For quantum states we use Dirac notation. A qubit with classical bit x encoded in basis b is written as $|\psi_x^b\rangle$. The set of bases is $\mathcal{B}$. In case of BB84 states we have $\mathcal{B} = \{x, z\}$; in case of 6-state encoding $\mathcal{B} = \{x, y, z\}$. The notation 'tr' stands for trace. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \text{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. States with non-italic label 'A', 'B' and 'E' indicate the subsystem of Alice/Bob/Eve.

Consider classical variables X, Y and a quantum system under Eve's control that depends on X and Y. The combined classical-quantum state is $\rho^{XYE} = \mathbb{E}_{xy} |xy\rangle\langle xy| \otimes \rho_{xy}^E$. The state of a sub-system is obtained by tracing out all the other subspaces, e.g. $\rho^{YE} = \text{tr}_X \rho^{XYE} = \mathbb{E}_y |y\rangle\langle y| \otimes \rho_y^E$, with $\rho_y^E = \mathbb{E}_x \rho_{xy}^E$. The fully mixed state on $\mathcal{H}_A$ is denoted as χ^A. We also use the notation $\mu^X = \mathbb{E}_x |x\rangle\langle x|$ for a classical variable X that is not necessarily uniform.

We write $\mathcal{S}(\mathcal{H})$ to denote the space of density matrices on Hilbert space $\mathcal{H}$, i.e. positive semi-definite operators acting on $\mathcal{H}$. Any quantum channel can be described by a completely positive trace-preserving (CPTP) map $\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ that transforms a mixed state ρ^A to ρ^B: $\mathcal{E}(\rho^A) = \rho^B$. For a map $\mathcal{E} : S(\mathcal{H}_A) \to S(\mathcal{H}_B)$, the notation $\mathcal{E}(\rho^{AC})$ stands for $(\mathcal{E} \otimes \mathbb{1}_C)(\rho^{AC})$, i.e. $\mathcal{E}$ acts only on the 'A' subsystem. Applying a map $\mathcal{E}_1$ and then $\mathcal{E}_2$ is written as the combined map $\mathcal{E}_2 \circ \mathcal{E}_1$. The diamond norm of $\mathcal{E}$ is defined as $\|\mathcal{E}\|_\diamond = \frac{1}{2} \sup_{\rho^{AC} \in \mathcal{S}(\mathcal{H}_{AC})} \|\mathcal{E}(\rho^{AC})\|_1$ with $\mathcal{H}_C$ an auxiliary system that can be considered to be of the same dimension as $\mathcal{H}_A$. The diamond norm $\|\mathcal{E} - \mathcal{E}'\|_\diamond$ can be used to bound the probability of distinguishing two CPTP maps $\mathcal{E}$ and $\mathcal{E}'$ given that the process is observed once. The maximum probability of a correct guess is $\frac{1}{2} + \frac{1}{4}\|\mathcal{E} - \mathcal{E}'\|_\diamond$. In quantum cryptography, one proof technique considers Alice and Bob performing actions on noisy EPR pairs. These actions are described by a CPTP map $\mathcal{E}$ acting on the input EPR states and outputting classical outputs for Alice and Bob, and correlated quantum side information for Eve. The security of such a protocol is quantified by the diamond norm between the actual map $\mathcal{E}$ and an idealised map $\mathcal{F}$ which produces perfectly behaving outputs (e.g. perfectly secret QKD keys). When $\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon$ we can consider $\mathcal{E}$ to behave ideally except with probability ε; this security metric is *composable* with other (sub-)protocols [21].

A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{T}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [24] if for all distinct pairs $x, x' \in \mathcal{X}$ and all pairs $y, y' \in \mathcal{T}$ it holds that $\text{Pr}_{h \in H}[h(x) = y \wedge h(x') = y'] = |\mathcal{T}|^{-2}$. Here the probability is over random $h \in H$. We define the rate of a quantum communication protocol as the number of message bits communicated per sent qubit.

3.2   Post-selection

For protocols that are invariant under permutation of their inputs it has been shown [6] that security against collective attacks (same attack applied to each qubit individually) implies security against general attacks, at the cost of extra privacy amplification. Let $\mathcal{E}$ be a protocol

that acts on $S(\mathcal{H}_{\mathrm{AB}}^{\otimes n})$ and let $\mathcal{F}$ be the perfect functionality of that protocol. If for all input permutations π there exists a map $\mathcal{K}_\pi$ on the output such that $\mathcal{E} \circ \pi = \mathcal{K}_\pi \circ \mathcal{E}$, then

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \quad \leq \quad (n+1)^{d^2-1} \max_{\sigma \in S(\mathcal{H}_{\mathrm{ABE}})} \left\|(\mathcal{E} - \mathcal{F})(\sigma^{\otimes n})\right\|_1 \tag{1}$$

where d is the dimension of the $\mathcal{H}_{\mathrm{AB}}$ space. ($d = 4$ for qubits). The product form $\sigma^{\otimes n}$ greatly simplifies the security analysis: now it suffices to prove security against 'collective' attacks, and to pay a price $2(d^2 - 1)\log(n+1)$ in the amount of privacy amplification, which is negligible compared to n.

3.3 Noise symmetrisation with random Pauli operators

In [19] it was shown that for n-EPR states in factorised form, as obtained from e.g. Post-selection, a further simplification is possible. For each individual qubit j, Alice and Bob apply the Pauli operation σ_{α_j} to their half of the EPR pair, with $\alpha_j \in \{0, 1, 2, 3\}$ random and public; then they forget α. The upshot is that Eve's state (the purification of the Alice+Bob system) is simplified to the 4×4 diagonal matrix $\mathrm{Diag}(1 - \frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2})$. Only one parameter is left over, the bit error probability γ caused by Eve. This symmetrisation trick is allowed when the *statistics* of the variables in the protocol is invariant under the Pauli operations.

4 Attacker model and security definitions

4.1 Attacker model

We work in same setting as Gottesman [9], as discussed in Section 1.3. We distinguish between on the one hand long-term secrets and on the other hand short-term secrets. A variable is considered short-term only if it is created[2] and immediately operated upon locally (without waiting for incoming communication), and then deleted. All other variables are long-term. (An example of a short-term variable is a nonce that is generated, immediately used a function evaluation and then deleted. On the other hand, all keys that are stored between protocol rounds are long-term.)
We consider two world views.

- **World1**. All secrets can be kept confidential indefinitely or destroyed.

- **World2**. Long-term secrets are in danger of leaking at some point in time.

There are several motivations for entertaining the second world view. (a) It is difficult to permanently erase data from nonvolatile memory. (b) Whereas everyone understands the necessity of keeping message content confidential, it is not easy to guarantee that protocol implementations (and users) handle the keys with the same care as the messages.
QKR protocols are typically designed to be secure in world1. In this paper we prove security guarantees that additionally hold in world2. One way of phrasing this is to say that we add 'user-proofness' to QKR.
Alice sends data to Bob in N chunks. We refer to the sending of one chunk as a 'round'.[3] In each round Bob tells Alice if he noticed a disturbance ('`reject`') or not ('`accept`'). In case of `reject` they are *alarmed* and they know that they must take special care to protect the

---

[2]Performing a measurement on a quantum state is also considered to 'create' a classical variable.
[3]One data transmission will be called a *pass*. A round consists of multiple passes.

keys of this round indefinitely (i.e. a fallback to *World1* security). Crucially, *we assume that a key theft occurring before the end of round N is immediately noticed by Alice and/or Bob.* Without this assumption it would be impossible to do Key Recycling in a meaningful way. We allow all keys to become public after round N.

The rest of the attacker model consists of the standard assumptions: no information, other than specified above, leaks from the labs of Alice and Bob; there are no side-channel attacks; Eve has unlimited (quantum) resources; all noise on the quantum channel is considered to be caused by Eve.

4.2 Security definitions

Let $\rho^{MK\tilde{K}TE} = \rho_{\texttt{accept}}^{MK\tilde{K}TE} + \rho_{\texttt{reject}}^{MK\tilde{K}TE}$ be the state after execution of a quantum encryption protocol, where M is the classical message, K stands for all the keys (and other long-term secrets), $\tilde{K}$ the updated keys, T the transcript observed by Eve, and E Eve's quantum side information. The two parts, associated with outcomes `accept` and `reject` respectively, are sub-normalized. In some existing QKR protocols, e.g. [12], the keys remain unchanged ($\tilde{K} = K$) in case of `accept`, whereas in other protocols, e.g. [14], there is always a key update. Alice and Bob share a 'reservoir' of key material from which key refreshes are done in case of `reject`.

The *Encryption* property (**ENC**) is defined as follows.

Definition 1 *An encryption scheme with output ρ^{MKTE} is called ε-encrypting (ε-ENC) if it satisfies*

$$\|\rho^{MTE} - \rho^M \otimes \rho^{TE}\|_1 \leq \varepsilon. \tag{2}$$

Furthermore we will work with the following definitions.

Definition 2 *A scheme with output $\rho^{MK\tilde{K}TE}$ is called ε-recycling (ε-KR) if (i) the reservoir is not accessed for creating the updated keys $\tilde{K}_{\texttt{accept}}$ and (ii) it satisfies*

$$\|\rho^{M\tilde{K}TE} - \rho^{\tilde{K}} \otimes \rho^{MTE}\|_1 \leq \varepsilon. \tag{3}$$

Definition 3 *A scheme with output $\rho^{MK\tilde{K}TE}$ is called ε-unclonable (ε-UE) if it satisfies*

$$\|\rho_{\texttt{accept}}^{MK\tilde{K}TE} - \rho^M \otimes \rho_{\texttt{accept}}^{K\tilde{K}TE}\|_1 \leq \varepsilon. \tag{4}$$

Note that other definitions exist. For instance, [12] has a recycling definition that allows Eve to have partial information about one of the keys (the measurement basis), as long as the min-entropy is high enough. Our preference for the above KR and UE definitions stems from (i) the fact that it allows for a unified treatment of all the keys; (ii) compatibility with the proof technique of [6, 19], which makes it possible to prove security of high-rate schemes. Furthermore our KR definition is compatible with [7]. Also note that our KR and UE do not automatically imply ENC. The ENC property has to be considered as a separate requirement. For the combination of ENC and KR we have the following two lemmas.

Lemma 1

$$\|\rho^{M\tilde{K}TE} - \rho^M \otimes \rho^{\tilde{K}} \otimes \rho^{TE}\|_1 \leq \varepsilon \quad \implies \quad \varepsilon\text{-ENC} \ \wedge \ 2\varepsilon\text{-KR} \tag{5}$$

6

Proof. Taking the lhs of (5) and tracing over $\tilde{K}$ yields ε-ENC. Furthermore, using the triangle inequality we write $\|\rho^{M\tilde{K}TE} - \rho^{\tilde{K}} \otimes \rho^{MTE}\|_1 \leq \|\rho^{M\tilde{K}TE} - \rho^M \otimes \rho^{\tilde{K}} \otimes \rho^{TE}\|_1 + \|\rho^M \otimes \rho^{\tilde{K}} \otimes \rho^{TE} - \rho^{\tilde{K}} \otimes \rho^{MTE}\|_1$. Both terms individually are bounded by ε by the lhs of (5); the first term directly, the second term after taking the $\tilde{K}$-trace. This proves 2ε-KR. $\qquad\square$

Lemma 2

$$(\tilde{K}_{\texttt{accept}} = K) \ \wedge \ \varepsilon_1\text{-}ENC \ \wedge \ \varepsilon_2\text{-}KR \quad \Longrightarrow \quad (\varepsilon_1 + \varepsilon_2)\text{-}UE. \tag{6}$$

Proof. With $\tilde{K}_{\texttt{accept}} = K$ we have $\|\rho^{MK\tilde{K}TE}_{\texttt{accept}} - \rho^M \otimes \rho^{K\tilde{K}TE}_{\texttt{accept}}\|_1 \leq \|\rho^{MKTE}_{\texttt{accept}} - \rho^M \otimes \rho^K \otimes \rho^{TE}_{\texttt{accept}}\|_1 + \|\rho^M \otimes \rho^K \otimes \rho^{TE}_{\texttt{accept}} - \rho^M \otimes \rho^{KTE}_{\texttt{accept}}\|_1$. The first term is bounded by taking the trace over K and using ε_1-ENC. For the second we take the trace over M, yielding $\|\rho^{KTE}_{\texttt{accept}} - \rho^K \otimes \rho^{TE}_{\texttt{accept}}\|_1$. This expression is bounded by ε_2, which is seen by taking the M-trace of (3). $\qquad\square$

Lemma 1 allows us to prove both ENC and KR by upperbounding a single quantity. Lemma 2 is an important statement: any ENC scheme that upon `accept` re-uses its keys *in unmodified form* and satisfies KR is automatically a UE scheme. It is interesting to note that [12] has $\tilde{K}_{\texttt{accept}} = K$ but does not satisfy KR, whereas [14, 15] satisfies KR but does not have $\tilde{K}_{\texttt{accept}} = K$. By Theorem 4 in [7] and Lemma 2, the *high-dimensional* scheme of Damgård et al. [7] has the UE property.

4.3   CPTP maps

We consider again the sequence of N chunks. The KR property must hold in the first $N-1$ rounds. The ENC and UE property must hold in all rounds. We write the statements of Section 4.2 in terms of CPTP maps, to make contact with the proof technique of Section 3.2. The different nature of the KR and UE property forces us to introduce two different notations for the CPTP map that is executed by Alice and Bob. On the one hand, we write $\mathcal{E}_{\text{KR}}$ for one round of the protocol, where at the end of the round the old keys (from the beginning of the round) are traced away. On the other hand, we write $\mathcal{E}_{\text{UE}}$ for one round without such a tracing operation. (The ENC property is not made explicit in this notation.) The following condition implies that the above given security properties hold except with probability ε,

$$\forall_{j \in \{1,\ldots,N\}} \quad \left\| \mathcal{E}^{(j)}_{\text{UE}} \circ \mathcal{E}^{(j-1)}_{\text{KR}} \circ \cdots \circ \mathcal{E}^{(1)}_{\text{KR}} - \mathcal{F}^{(j)}_{\text{UE}} \circ \mathcal{F}^{(j-1)}_{\text{KR}} \circ \cdots \circ \mathcal{F}^{(1)}_{\text{KR}} \right\|_\diamond \leq \varepsilon, \tag{7}$$

where the superscript is the round index, and $\mathcal{F}$ stands for the idealized version of the protocol. We can arrive at a simplified statement using the following lemma.

Lemma 3 *For any CPTP maps $\mathcal{A}, \mathcal{A}', \mathcal{B}, \mathcal{B}'$, it holds that*

$$\|\mathcal{A} \circ \mathcal{B} - \mathcal{A}' \circ \mathcal{B}'\|_\diamond \ \leq \ \|\mathcal{A} - \mathcal{A}'\|_\diamond + \|\mathcal{B} - \mathcal{B}'\|_\diamond. \tag{8}$$

Proof:

$$\|\mathcal{A} \circ \mathcal{B} - \mathcal{A}' \circ \mathcal{B}'\|_\diamond \ = \ \|\mathcal{A} \circ \mathcal{B} - \mathcal{A}' \circ \mathcal{B}' + \mathcal{A}' \circ \mathcal{B} - \mathcal{A}' \circ \mathcal{B}\|_\diamond \tag{9}$$
$$\leq \ \|(\mathcal{A} - \mathcal{A}') \circ \mathcal{B}\|_\diamond + \|\mathcal{A}' \circ (\mathcal{B} - \mathcal{B}')\|_\diamond \tag{10}$$
$$\leq \ \|\mathcal{A} - \mathcal{A}'\|_\diamond + \|\mathcal{B} - \mathcal{B}'\|_\diamond \tag{11}$$

where the last inequality holds because a CPTP map can never increase the trace distance. $\square$

Using Lemma 3 it is easily seen that the following condition implies (7),

$$(N-1)\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_\diamond + \|\mathcal{E}_{\mathrm{UE}} - \mathcal{F}_{\mathrm{UE}}\|_\diamond \leq \varepsilon. \tag{12}$$

It is therefore sufficient to upper bound the single-round quantities $\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_\diamond$ and $\|\mathcal{E}_{\mathrm{UE}} - \mathcal{F}_{\mathrm{UE}}\|_\diamond$. The ideal mapping $\mathcal{F}$ is obtained from $\mathcal{E}$ as follows. From $\mathcal{E}(\rho^{\mathrm{ABE}})$ one traces out those classical variables that are supposed to remain unknown to Eve, and takes a tensor product with an isolated mixed state of these variables. In the case of $\mathcal{E}_{\mathrm{KR}}$ the relevant variables are the message m and the next-round keys, which we denote here as $\tilde{k}$. In the case of $\mathcal{E}_{\mathrm{UE}}$ it is only the message, and only the `accept` part of the mapping is relevant. (Upon `reject` the functionality of $\mathcal{E}_{\mathrm{UE}}$ is ideal by definition.) Hence we have

$$\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_\diamond = \frac{1}{2}\sup_{\rho^{\mathrm{ABE}}}\left\|\mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) - \operatorname*{\mathbb{E}}_{m\tilde{k}}|m\tilde{k}\rangle\langle m\tilde{k}| \otimes \operatorname{tr}_{M\tilde{K}}\mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}})\right\|_1 \tag{13}$$

$$\|\mathcal{E}_{\mathrm{UE}} - \mathcal{F}_{\mathrm{UE}}\|_\diamond = \frac{1}{2}\sup_{\rho^{\mathrm{ABE}}}\left\|\mathcal{E}_{\mathrm{UE}}^{\texttt{accept}}(\rho^{\mathrm{ABE}}) - \operatorname*{\mathbb{E}}_{m}|m\rangle\langle m| \otimes \operatorname{tr}_M \mathcal{E}_{\mathrm{UE}}^{\texttt{accept}}(\rho^{\mathrm{ABE}})\right\|_1, \tag{14}$$

where in (14) the `reject` part vanishes as we have implicitly assumed that $\mathcal{E}$ has ideal functionality in the `reject` case, i.e. ENC holds.

5 The proposed scheme, `KRUE`

We propose a qubit-based prepare-and-measure scheme for Unclonable Encryption with Key Recycling. We will refer to it as `KRUE`.

5.1 Pairwise independent hashing with easy inversion

We will need the privacy amplification step to be easily computable in two directions. Unfortunately the code-based construction due to Gottesman [9] does not work with the proof technique of [19], which requires a family of universal hash functions. We will be using a family of invertible functions $F : \{0,1\}^\nu \to \{0,1\}^\nu$ that has the collision properties of a pairwise independent hash function. An easy way to construct such a family is to use multiplication in $GF(2^\nu)$. Let $u \in GF(2^\nu)$ be randomly chosen. Define $F_u(x) = u \cdot x$, where the multiplication is in $GF(2^\nu)$. A pairwise independent family of hash functions Φ from $\{0,1\}^\nu$ to $\{0,1\}^\ell$, with $\ell \leq \nu$, is implemented by taking the ℓ most significant bits of $F_u(x)$. We denote this as

$$\Phi_u(x) = F_u(x)[:\ell]. \tag{15}$$

The inverse operation is as follows. Given $c \in \{0,1\}^\ell$, generate random $r \in \{0,1\}^{\nu-\ell}$ and output $F_u^{\mathrm{inv}}(c\|r)$. It obviously holds that $\Phi_u(F_u^{\mathrm{inv}}(c\|r)) = c$. Computing an inverse in $GF(2^\nu)$ costs $O(\nu \log^2 \nu)$ operations [17].

5.2 Protocol steps

Alice and Bob have agreed on a MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^{\ell-\lambda} \to \{0,1\}^\lambda$, the function families F and Φ as discussed in Section 5.1, with $\nu = k$, and a linear error correcting code which has encoding function $\mathrm{Enc} : \{0,1\}^k \to \{0,1\}^n$ in systematic form and decoding $\mathrm{Dec} : \{0,1\}^n \to \{0,1\}^k$.

In round j, Alice wants to send a message $\mu_j \in \{0,1\}^{\ell-(n-k)-2\lambda-1}$. We will often drop the index j for notational brevity. The key material shared between Alice and Bob consists

8

of a mask $z \in \{0,1\}^{\ell}$, a MAC key $k_{\text{MAC}} \in \{0,1\}^{\lambda}$, a basis sequence $b \in \mathcal{B}^n$, a MAC key $k_{\text{fb}} \in \{0,1\}^{\lambda}$ for the feedback bit, a one-time pad $k_{\text{OTP}} \in \{0,1\}$ for the feedback bit, a key $u \in \{0,1\}^k$ for universal hashing and a key $e \in \{0,1\}^{n-k}$ to mask the redundancy bits. They have a reservoir of spare key material (k_{rej}) from which to refresh their keys in case of `reject`. In each round Alice and Bob perform the following steps (see Fig. 1):

Encryption:

Alice generates random strings $\kappa \in \{0,1\}^{\lambda+1+n-k}$ and $r \in \{0,1\}^{k-\ell}$. She computes the authentication tag $\tau = \Gamma(k_{\text{MAC}}, \mu\|\kappa)$, the augmented message $m = \mu\|\kappa\|\tau$, the ciphertext $c = z \oplus m$, the reversed privacy amplification $p = F_u^{\text{inv}}(c\|r) \in \{0,1\}^k$ and the qubit payload $x = \text{Enc}(p) \oplus (\vec{0}^k\|e) \in \{0,1\}^n$. She prepares $|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_{x_i}^{b_i}\rangle$ and sends it to Bob.

Decryption:

Bob receives $|\Psi\rangle'$. He measures $|\Psi\rangle'$ in the basis b. The result is $x' \in \{0,1\}^n$. He decodes $\hat{p} = \text{Dec}(x' \oplus (\vec{0}_k\|e))$. He computes $\hat{c} = \Phi_u(\hat{p})$ and $\hat{\mu}\|\hat{\kappa}\|\hat{\tau} = \hat{c} \oplus z$. He sets $\omega = 1$ (`accept`) if $\Gamma(k_{\text{MAC}}, \hat{\mu}\|\hat{\kappa}) == \hat{\tau}$, otherwise $\omega = 0$ (`reject`). He computes $\tau_{\text{fb}} = \Gamma(k_{\text{fb}}, \omega \oplus k_{\text{OTP}})$ and sends $\omega \oplus k_{\text{OTP}}$ and τ_{fb} to Alice.

Key Update:

Alice and Bob perform the following actions (a tilde denotes the key for the next round):

In case of `accept`: Re-use b, u, k_{MAC}, z. Set next round keys: $(\tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}) = \kappa$.

In case of `reject`: Re-use b, u, k_{MAC}. Take fresh $\tilde{z}, \tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}$ from k_{rej}.
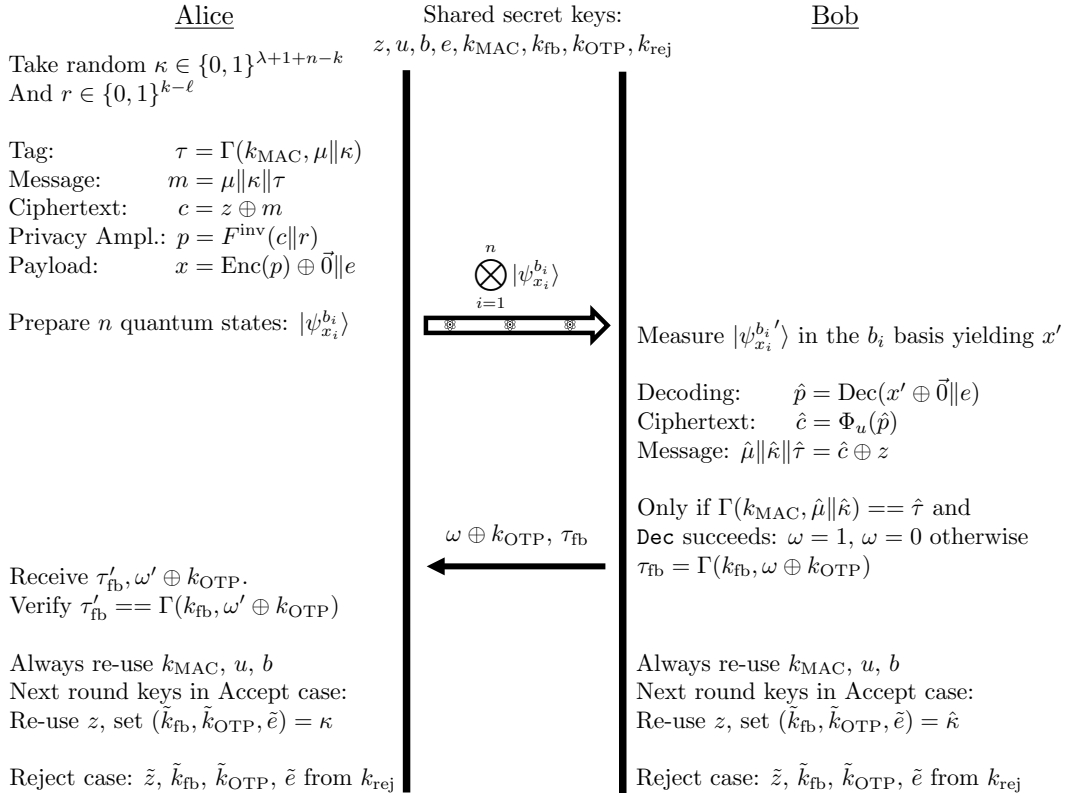

Alice	Shared secret keys:	Bob
	$z, u, b, e, k_{\text{MAC}}, k_{\text{fb}}, k_{\text{OTP}}, k_{\text{rej}}$	

Take random $\kappa \in \{0,1\}^{\lambda+1+n-k}$
And $r \in \{0,1\}^{k-\ell}$

Tag: $\quad\quad\quad \tau = \Gamma(k_{\text{MAC}}, \mu\|\kappa)$
Message: $\quad\quad m = \mu\|\kappa\|\tau$
Ciphertext: $\quad c = z \oplus m$
Privacy Ampl.: $p = F^{\text{inv}}(c\|r)$
Payload: $\quad\quad x = \text{Enc}(p) \oplus \vec{0}\|e$

Prepare n quantum states: $|\psi_{x_i}^{b_i}\rangle$

$\bigotimes_{i=1}^{n} |\psi_{x_i}^{b_i}\rangle$

Measure $|\psi_{x_i}^{b_i}{}'\rangle$ in the b_i basis yielding x'

Decoding: $\quad \hat{p} = \text{Dec}(x' \oplus \vec{0}\|e)$
Ciphertext: $\quad \hat{c} = \Phi_u(\hat{p})$
Message: $\hat{\mu}\|\hat{\kappa}\|\hat{\tau} = \hat{c} \oplus z$

Only if $\Gamma(k_{\text{MAC}}, \hat{\mu}\|\hat{\kappa}) == \hat{\tau}$ and
`Dec` succeeds: $\omega = 1$, $\omega = 0$ otherwise
$\tau_{\text{fb}} = \Gamma(k_{\text{fb}}, \omega \oplus k_{\text{OTP}})$

$\omega \oplus k_{\text{OTP}}, \tau_{\text{fb}}$

Receive $\tau_{\text{fb}}', \omega' \oplus k_{\text{OTP}}$.
Verify $\tau_{\text{fb}}' == \Gamma(k_{\text{fb}}, \omega' \oplus k_{\text{OTP}})$

Always re-use k_{MAC}, u, b
Next round keys in Accept case:
Re-use z, set $(\tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}) = \kappa$

Always re-use k_{MAC}, u, b
Next round keys in Accept case:
Re-use z, set $(\tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}) = \hat{\kappa}$

Reject case: $\tilde{z}, \tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}$ from k_{rej}

Reject case: $\tilde{z}, \tilde{k}_{\text{fb}}, \tilde{k}_{\text{OTP}}, \tilde{e}$ from k_{rej}

Figure 1: *Protocol steps of a single round.*

After round N, according to the attacker model, all keys from all rounds leak[4] except for

---

[4]Optionally this leakage can be made part of the protocol, i.e. Alice and Bob publish the keys.

masks z associated with `reject` events. I.e. what leaks is: $b, u, k_{\mathrm{MAC}}, \{k_{\mathrm{fb}}^{(j)}, k_{\mathrm{OTP}}^{(j)}, e^{(j)}\}_{j=1}^N$, and if round N was `accept` also $z^{(N)}$.

Remarks:

- The augmented message m contains the three keys $\tilde{k}_{\mathrm{fb}}, \tilde{k}_{\mathrm{OTP}}, \tilde{e}$ for the next round. This means that qubits are 'spent' in order to send something other than μ, which reduces the communication rate. Here the mask $e \in \{0,1\}^{n-k}$ for the redundancy bits is the dominant part; its size is asymptotically $nh(\beta)$ bits, giving rise to a rate penalty term $h(\beta)$ familiar from QKD.

- The `accept`/`reject` feedback bit is encrypted, which temporarily prevents Eve from gaining information from 'oracle' access to the feedback. This allows us to re-use b in unmodified form after `accept`.

- Even in the case of known plaintext, from Eve's point of view the 'payload' $x \in \{0,1\}^n$ in the state $\bigotimes_{i=1}^n |\psi_{x_i}^{b_i}\rangle$ is uniformly distributed. The z masks ℓ bits; then appending r increases that to k bits; finally the e masks the $n-k$ redundancy bits.

5.3 EPR version of the protocol

We will base the security proof on the EPR version of the protocol, making use of Post-selection (Section 3.2) and the random-Pauli noise symmetrisation technique (Section 3.3).

n noisy singlet states are produced by an untrusted source, e.g. Eve. One half of each EPR pair is sent to Alice, the other half to Bob. Alice and Bob apply the random Pauli operations as described in Section 3.3. Then Alice measures her qubits in the bases $b \in \mathcal{B}^n$ resulting in a string $s \in \{0,1\}^n$. Bob too measures his qubits in basis b, which yields $t \in \{0,1\}^n$. Alice computes x as specified in Section 5.2, then computes $a = x \oplus s$ and sends a to Bob over an authenticated classical channel. Bob receives a, computes $x' = \bar{t} \oplus a$ and performs the decryption steps specified in Section 5.2.

We are allowed to use Post-selection because our protocol is invariant under permutation of the EPR pairs. A permutation re-arranges the noise in the observed strings s and t over the bit positions $\{1, \ldots, n\}$; however, the error correction step is insensitive to such a change. The use of the noise symmetrisation technique is allowed because the statistics is invariant under the Pauli operations. In the case of BB84 encoding and 6-state encoding, the Paulis cause bit flips in the string $x \in \{0,1\}^n$ in positions known to Alice and Bob, which does not change the protocol in any essential way.[5] Security of the EPR version implies security of the prepare-and-measure protocol of Section 5.2.

6 Security proof for the EPR verison of the protocol

6.1 CPTP maps

We now specify the exact form of the CPTP map which represents one round. We start with $\mathcal{E}_{\mathrm{UE}}$ and write $\mathcal{E}_{\mathrm{KR}} = \mathcal{T}_{\mathrm{KR}} \circ \mathcal{E}_{\mathrm{UE}}$, where $\mathcal{T}_{\mathrm{KR}}$ is a partial trace operation. The $\mathcal{E}_{\mathrm{UE}}$ can be viewed as four consecutive maps: an initialization step $\mathcal{I}$ where the input variables are prepared; a measurement step $\mathcal{M}$; a post-processing step $\mathcal{P}$ representing all further computations; a

---

[5]In 8-state encoding [23], applying a Pauli changes the basis b in a way known to Alice and Bob. Again, this does not affect the security.

partial trace step $\mathcal{T}_{\mathrm{UE}}$ where all variables that are not part of the output or the transcript are traced away,

$$\mathcal{E}_{\mathrm{UE}} = \mathcal{T}_{\mathrm{UE}} \circ \mathcal{P} \circ \mathcal{M} \circ \mathcal{I}. \tag{16}$$

The initialization merely appends the input variables,

$$\mathcal{I}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbzue} |mbzue\rangle\langle mbzue| \otimes \rho^{\mathrm{ABE}}. \tag{17}$$

Here b, z, u, e are uniform, but m not necessarily. The measurement acts on the b-space and ρ^{ABE}, outputting the strings s, t and Eve's state ρ^{E}_{bst}, which is correlated to the measurement basis b and the outcomes s, t,

$$\mathcal{M}(|b\rangle\langle b| \otimes \rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{st} |bst\rangle\langle bst| \otimes \rho^{\mathrm{E}}_{bst}. \tag{18}$$

Here the distribution of s and t is governed by the i.i.d. noise with noise parameter γ. The marginals of s and t are uniform, while for all $j \in \{1, \ldots, n\}$ it holds that $\Pr[s_j = t_j] = \gamma$. In the post-processing the flag ω is computed as a function of s and t which we will denote as θ_{st}. Let $n\beta$ be the number of errors that can be corrected by the error-correcting code. Then

$$\theta_{st} = \begin{cases} 1 & \text{if } |\bar{s} \oplus t| \leq n\beta \\ 0 & \text{if } |\bar{s} \oplus t| > n\beta \end{cases}. \tag{19}$$

We will use the notation $P_{\mathrm{corr}}(n, \beta, \gamma)$ for the probability of the event $\theta_{st} = 1$.

$$P_{\mathrm{corr}}(n, \beta, \gamma) \overset{\mathrm{def}}{=} \mathop{\mathbb{E}}_{st} \theta_{st} = \sum_{c=0}^{\lfloor n\beta \rfloor} \binom{n}{c} \gamma^c (1 - \gamma)^{n-c}. \tag{20}$$

The result of applying $\mathcal{I}, \mathcal{M}, \mathcal{P}$ is given by

$$(\mathcal{P} \circ \mathcal{M} \circ \mathcal{I})(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbzuest} |mbzuest\rangle\langle mbzuest| \otimes \rho^{\mathrm{E}}_{bst} \otimes \sum_{capxx'\omega\tilde{z}} \mathop{\mathbb{E}}_{r} |capxx'\omega\tilde{z}r\rangle\langle capxx'\omega\tilde{z}r|$$

$$\delta_{a, s\oplus x} \delta_{c, m\oplus z} \delta_{p, F_u^{\mathrm{inv}}(c\|r)} \delta_{x, p\|[\mathrm{Red}(p)\oplus e]} \delta_{x', \bar{t}\oplus a} \delta_{\omega, \theta_{st}} \left[\omega \delta_{\tilde{z}z} + \frac{\overline{\omega}}{2^\ell} \right]. \tag{21}$$

Here r is uniform and 'Red(p)' stands for the redundancy bits appended to p in the systematic-form ECC encoding Enc(p). In the final step $\mathcal{T}_{\mathrm{UE}}$ we trace away all variables that are not part of the transcript or the output: s, t, c, p, x, x', r. These variables exist only temporarily and can be quickly discarded by Alice and Bob; they are never stored in nonvolatile memory. The a and ω are observed by Eve as part of the communication. (The ω in encrypted form, but the key is assumed to leak in the future.) The b, z, u, e are assumed to leak in the future and thus they have to be kept as part of the state. We obtain[6]

$$\mathcal{E}_{\mathrm{UE}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}\omega} |mbzuea\tilde{z}\omega\rangle\langle mbzuea\tilde{z}\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\mathrm{E}}_{bst} \sum_p 2^\ell \delta_{\Phi_u(p), m\oplus z}$$

$$2^{-k} \delta_{s\oplus a, p\|[\mathrm{Red}(p)\oplus e]} \delta_{\omega, \theta_{st}} \left[\omega \delta_{\tilde{z}z} + \overline{\omega} 2^{-\ell} \right]. \tag{22}$$

---

[6] Note that tracing out u or $z\tilde{z}$ in (22) yields a state in which the m-subspace is completely decoupled from the rest of the Hilbert space. This shows that the scheme, when merely viewed as an encryption scheme, protects m unconditionally as soon as the adversary does not know u or $z\tilde{z}$.

As discussed in Section 4, only the `accept` part (the $\omega = 1$ part) of the idealized $\mathcal{F}_{\text{UE}}$ is relevant. This is obtained as $\mathcal{F}_{\text{UE}}^{\text{accept}}(\rho^{\text{ABE}}) = \mathbb{E}_m |m\rangle\langle m| \otimes \text{tr}_M \mathcal{E}_{\text{UE}}^{\text{accept}}(\rho^{\text{ABE}})$. We get

$$\mathcal{F}_{\text{UE}}^{\text{accept}}(\rho^{\text{ABE}}) = \underset{mbzue}{\mathbb{E}} \sum_{a\tilde{z}} |mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z}$$
$$\otimes \underset{st}{\mathbb{E}}\, \rho_{bst}^{\text{E}}\theta_{st} \sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[\text{Red}(p)\oplus e]} \underset{m'}{\mathbb{E}}\,\delta_{\Phi_u(p),m'\oplus z}. \tag{23}$$

Note that this expression is sub-normalized; its trace equals P_{corr}. We write

$$(\mathcal{E}_{\text{UE}}^{\text{accept}} - \mathcal{F}_{\text{UE}}^{\text{accept}})(\rho^{\text{ABE}}) = \underset{mbzue}{\mathbb{E}} \sum_{a\tilde{z}} |mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z}$$
$$\otimes \underset{st}{\mathbb{E}}\, \rho_{bst}^{\text{E}}\theta_{st} \sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[\text{Red}(p)\oplus e]}[\delta_{\Phi_u(p),m\oplus z} - \underset{m'}{\mathbb{E}}\,\delta_{\Phi_u(p),m'\oplus z}]. \tag{24}$$

For the description of $\mathcal{E}_{\text{KR}}$ we have to take (22) and trace out z,e,ω.

$$\mathcal{E}_{\text{KR}}(\rho^{\text{ABE}}) = \underset{mbu}{\mathbb{E}}\, 2^{-n} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \underset{st}{\mathbb{E}}\, \rho_{bst}^{\text{E}}\Big[\theta_{st}\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde{z}} + 2^{-\ell}\overline{\theta_{st}}\Big]. \tag{25}$$

The ideal functionality $\mathcal{F}_{\text{KR}}$ has $m,b,u,\tilde{z}$ decoupled from the rest of the system. We have $\mathcal{F}_{\text{KR}}(\rho^{\text{ABE}}) = \mathbb{E}_{mbu} 2^{-\ell} \sum_{\tilde{z}} |mbu\tilde{z}\rangle\langle mbu\tilde{z}| \otimes \text{tr}_{MBU\tilde{Z}}\mathcal{E}_{\text{KR}}(\rho^{\text{ABE}})$, which yields

$$\mathcal{F}_{\text{KR}}(\rho^{\text{ABE}}) = \underset{mbu}{\mathbb{E}}\, 2^{-n-\ell} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \underset{st}{\mathbb{E}}\, \underset{b'}{\mathbb{E}}\, \rho_{b'st}^{\text{E}}. \tag{26}$$

Note that $\mathbb{E}_{st} \mathbb{E}_{b'} \rho_{b'st}^{\text{E}} = \rho^{\text{E}}$.

Lemma 4 *Let ρ^{ABE} denote the purification of a 4^n-dimensional state ρ^{AB}. Let $b \in \mathcal{B}^n$ be a qubit-wise orthonormal basis. It holds that $\rho_b^{\text{E}} = \rho^{\text{E}}$.*

Proof: Let P_{bs}^{A} denote a projection operator on subsystem 'A' corresponding to a measurement in basis b with outcome $s \in \{0,1\}^n$. We have $\rho_b^{\text{E}} \stackrel{\text{def}}{=} \mathbb{E}_{st} \rho_{bst}^{\text{E}} = \sum_{st} \text{tr}_{\text{AB}}(P_{bs}^{\text{A}} \otimes P_{bt}^{\text{B}} \otimes \mathbb{1})\rho^{\text{ABE}}$ $= \text{tr}_{\text{AB}}([\sum_s P_{bs}^{\text{A}}] \otimes [\sum_t P_{bt}^{\text{B}}] \otimes \mathbb{1})\rho^{\text{ABE}} = \rho^{\text{E}}$. We use the fact that $\sum_s P_{bs}^{\text{A}} = \mathbb{1}$ and $\sum_t P_{bt}^{\text{B}} = \mathbb{1}$ for any b. $\qquad\square$

Lemma 4 allows us to write

$$(\mathcal{E}_{\text{KR}} - \mathcal{F}_{\text{KR}})(\rho^{\text{ABE}}) = \underset{mbu}{\mathbb{E}}\, 2^{-n-\ell} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \underset{st}{\mathbb{E}}\, \rho_{bst}^{\text{E}}\theta_{st}[2^\ell\delta_{\Phi_u((s\oplus a)[:k]),m\oplus\tilde{z}} - 1]. \tag{27}$$

6.2 Intermezzo: QKD asymptotics

In Appendix A, we consider a version of QKD where privacy amplification is implemented as in Section 5.2, and the syndrome is sent to Bob in OTP'ed form; we show that this leads to a bound of the form

$$\|\mathcal{E}_{\text{QKD}} - \mathcal{F}_{\text{QKD}}\|_\diamond \leq \tfrac{1}{2} \underset{mbu}{\mathbb{E}}\, \frac{1}{2^{n+\ell}} \sum_{ac} \left\| \underset{st}{\mathbb{E}}\, \rho_{bst}^{\text{E}}\theta_{st}2^\ell[\delta_{c,m\oplus\Phi_u(a\oplus s)} - \underset{m'}{\mathbb{E}}\,\delta_{c,m'\oplus\Phi_u(a\oplus s)}] \right\|_1, \tag{28}$$

which after some algebra gives rise to

$$\|\mathcal{E}_{\text{QKD}} - \mathcal{F}_{\text{QKD}}\|_\diamond \leq \min\left(P_{\text{corr}}, \frac{1}{2} \underset{b}{\mathbb{E}}\, \text{tr} \sqrt{2^\ell \underset{ss'}{\mathbb{E}}\, \delta_{ss'}\rho_{bs}^{\text{E}}\rho_{bs'}^{\text{E}}}\right), \tag{29}$$

12

and that from (29) the well known asymptotic QKD rates is obtained: $1 - 2h(\beta)$ for BB84 and $1 - h(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$ for 6-state QKD. If the syndrome ($\sigma = \text{Syn } x$) is sent in the clear, the right hand side of (28) acquires an extra $\sum_\sigma$ outside the trace norm and a factor $\delta_{\sigma, \text{Syn}(s \oplus a)}$ inside the trace norm; the effect on (29) is an extra factor 2^{n-k} under the square root; while this alteration reduces the threshold value $\ell_{\max}$ by an amount $n - k$, it has no effect on the rate since OTP'ing the syndrome would incur a penalty of exactly the same size.

6.3 Achievable rate

In the analysis we do not explicitly write down contributions from the authentication failure probability. It is implicit that each MAC adds a term $2^{-\lambda}$ to the overall security parameter.

Theorem 1 *The* KRUE *protocol satisfies the ENC, KR and UE properties as defined in Section 4 while achieving the following asymptotic rate,*

$$r_{4\text{state}} = 1 - 3h(\beta) \quad ; \quad r_{6\text{state}} = 1 - h(1 - \tfrac{3\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}) - h(\beta). \tag{30}$$

In other words, the achievable rate is worse than the QKD rate by a term $h(\beta)$.

Proof of Theorem 1: Because of the inclusion of $n - k + \lambda + 1$ extra bits in the augmented message m, the asymptotic rate of the protocol is $\ell_{\max}/n - h(\beta)$. We need to determine the value of $\ell_{\max}$ for both the UE and KR property separately and take the smaller of the two. **Part 1**. First we note that (24) is the difference of two sub-normalised states that both have trace equal to P_{corr}. This immediately yields the bound $\|\mathcal{E}_{\text{UE}} - \mathcal{F}_{\text{UE}}\|_\diamond \leq P_{\text{corr}}$. Furthermore, from (24) we get

$$\|\mathcal{E}_{\text{UE}} - \mathcal{F}_{\text{UE}}\|_\diamond = \mathop{\mathbb{E}}_{mbzue} \frac{1}{2^n} \sum_a \left\| \mathop{\mathbb{E}}_{st} \rho_{bst}^{\text{E}} \theta_{st} \sum_p 2^{\ell+n-k} \delta_{s \oplus a, p \| [\text{Red}(p) \oplus e]} \left[\delta_{\Phi_u(p), m \oplus z} - \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(p), m' \oplus z} \right] \right\|_1 \tag{31}$$

which resembles (28). The main difference is the $2^{n-k} \sum_p \delta_{s \oplus a, p \| [\text{Red}(p) \oplus e]}$. In the derivation as shown in Appendix A, upon doubling as in (44) applying the $\mathbb{E}_u$ then yields instead of $\delta_{ss'}$ the following expression,

$$(2^{n-k})^2 \sum_{pp'} \delta_{pp'} \delta_{s \oplus a, p \| (e \oplus \text{Red} p)} \delta_{s' \oplus a, p' \| (e \oplus \text{Red} p')} = (2^{n-k})^2 \delta_{ss'} \delta_{e, (s \oplus a)[k+1:n] \oplus \text{Red}((s \oplus a)[:k])}. \tag{32}$$

The factor $(2^{n-k})^2 \delta_{e, \cdots}$, together with the $\mathbb{E}_e$ outside the trace norm, together have the same effect as having the plaintext syndrome in the QKD derivation: a factor 2^{n-k} under the square root in (29). Asymptotically this yields $\ell_{\max}^{\text{uncl,4state}} = n - 2nh(\beta)$ and $\ell_{\max}^{\text{uncl,6state}} = n - nh(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$.
Part 2. First we note that (27) is the difference of two sub-normalised states that both have trace equal to P_{corr}. This immediately yields the bound $\|\mathcal{E}_{\text{KR}} - \mathcal{F}_{\text{KR}}\|_\diamond \leq P_{\text{corr}}$. Furthermore, from (27) we find

$$\|\mathcal{E}_{\text{KR}} - \mathcal{F}_{\text{KR}}\|_\diamond = \frac{1}{2} \mathop{\mathbb{E}}_{mbu} \frac{1}{2^{n+\ell}} \sum_{a\tilde{z}} \left\| \mathop{\mathbb{E}}_{st} \rho_{bst}^{\text{E}} \theta_{st} [2^\ell \delta_{\Phi_u((s \oplus a)[:k]), m \oplus \tilde{z}} - 1] \right\|_1. \tag{33}$$

This expression very closely resembles (28), with $\tilde{z}$ precisely playing the role of c, and the term $\mathbb{E}_{m'} \delta_{c, m' \oplus \Phi_u(a \oplus s)}$ replaced by the constant '1'. Carrying the '1' through steps (44) and further in Appendix A yields the same result as the QKD derivation, except for one

13

important difference: the $(s + a)[:k]$ restriction to the first k bits yields a modification of $\delta_{ss'}$ to the first k bits only. In the end result the parameter n is entirely replaced by k. Hence we obtain asymptotically $\ell_{\max}^{\text{KR,4state}} = k - kh(\beta) = n(1 - h(\beta))^2$ and $\ell_{\max}^{\text{KR,6state}} = k + kh(\beta) - kh(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}) = n[1 - h(\beta)][1 + h(\beta) - h(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})]$.

It is easily seen that $\ell_{\max}^{\text{UE}} \leq \ell_{\max}^{\text{KR}}$. For brevity we use shorthand notation $h = h(\beta)$ and $H = h(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$, noting that $H > h$ and $H < 2h$. For BB84 encoding we see $\ell_{\max}^{\text{KR}}/\ell_{\max}^{\text{UE}} = \frac{(1-h)^2}{1-2h} \geq 1$. For 6-state we see $\ell_{\max}^{\text{KR}}/\ell_{\max}^{\text{UE}} = \frac{(1-h)(1+h-H)}{1-H} = \frac{1-H+h(H-h)}{1-H} \geq 1$. $\square$

Remark: In the zero-noise case ($\beta = 0$) there is no syndrome mask e. Then we have, without inequalities,
$$\|\mathcal{E}_{\text{UE}} - \mathcal{F}_{\text{UE}}\|_\diamond = \|\mathcal{E}_{\text{KR}} - \mathcal{F}_{\text{KR}}\|_\diamond = \|\mathcal{E}_{\text{QKD}} - \mathcal{F}_{\text{QKD}}\|_\diamond = \mathbb{E}_{mubza} \| \mathbb{E}_{st} \theta_{st} \rho_{bst}^{\text{E}} [2^\ell \delta_{\Phi_u(s \oplus a), m \oplus z} - 1] \|_1,$$
i.e. the security of QKD immediately implies UE and KR.

Also note that for $\beta = 0$ we can invoke Lemma 2 to prove UE; we can view the keys k_{fb} and k_{OTP} as 'external' to the proof, e.g. replace k_{fb} by the existence of an authenticated channel and *spend* one bit to mask the feedback ω.

For $\beta > 0$ we are not allowed to invoke Lemma 2, since not all the key material is carried to the next round in unmodified form: upon `accept` the e is updated. The e plays an integral role in the bounding of the diamond norm (31) and cannot be moved outside that part of the proof.

7 Combining protocols

In the protocol as detailed in Section 5, the key $\tilde{e}_{\text{accept}}$ is transported in an UE manner. This is in a sense 'overkill' since the attacker model assumes that long-term keys such as $\tilde{e}$ will leak eventually. In this section we explore alternative ways of transporting $\tilde{e}_{\text{accept}}$ which yield a better rate. We consider only large-message asymptotics.

We introduce the following modified protocol, which we will refer to as KRUE*. The message m (Fig.1) now contains μ but not κ. The κ is received in a different manner, but still together with the qubits of the KRUE* scheme. Ignoring the missing κ, the asymptotic rate of KRUE* itself equals the QKD rate: $r_4^{\text{KRUE}^*} = 1 - 2h(\beta)$ for 4-state encoding and $r_6^{\text{KRUE}^*} = 1 - h(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$ for 6-state encoding.

7.1 Combining KRUE* with QKD

Here we consider KRUE* where κ is received One-Time-Padded over the classical channel, and the OTP key comes from running QKD[7] before KRUE*. Compared to our original scheme KRUE, the net difference is:

- Increased round complexity. Even assuming the most efficient form of QKD, Alice needs at least one extra pass to Bob. The KRUE* qubits cannot be sent in the same pass as the QKD qubits, since QKD requires Bob to respond to Alice before the QKD key can be estabished.

- Better rate. The asymptotic rate is $r_4^{\text{QKD+KRUE}^*} = \frac{[1-2h(\beta)]^2}{1-h(\beta)}$ for 4-state encoding and $r_6^{\text{QKD+KRUE}^*} = \frac{[1-h(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})]^2}{1-h(1-\frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})+h(\beta)}$ for 6-state. This can be seen as follows. Let $\mu \in \{0,1\}^L$. Sending μ via KRUE* needs $n = L/r^{\text{KRUE}^*}$ qubits. The size of the syndrome is $nh(\beta)$.

---

[7]In case of QKD failure, Alice and Bob try QKD again. It does not matter if Eve observes the number of QKD failures.

Creating the OTP key using QKD takes $nh(\beta)/r^{\mathrm{QKD}}$ qubits. The total number of qubits is $L(r^{\mathrm{QKD}} + h(\beta))/(r^{\mathrm{QKD}})^2$.

The combined scheme has the UE property regarding the message μ. First, by composability it is safe to use the QKD key in any manner. Second, by the UE property of KRUE*, μ is secure even if all keys, including everything contained in κ, eventually leak.

Interestingly, the rate $r_4^{\mathrm{QKD+KRUE}^*}$ that we achieve here is twice the rate of QKD followed by Gottesman's Unclonable Encryption scheme [9].[8]

7.2 Combining KRUE* with QKR

Now Bob receives κ via the 'Quantum Alice and Silent Bob' QKR scheme [14]. Again, in case of QKR failure Alice and Bob can just keep trying the QKR until it succeeds. (This is the case because the only purpose is to transport random keys for the next round.) The scheme of [14] has the following properties, (i) its asymptotic rate equals the QKD rate; (ii) Alice sends only qubits and no classical communication.
The advantage of using QKR over QKD is that *everything can be sent in the same pass.* Hence the combination KRUE*+QKR achieves the same rate as KRUE*+QKD but has better round complexity (only one pass from Alice).

Theorem 2 *Let P_{KR} be a ε_1-KR scheme in which Alice makes one pass. Let P_{UE} be a ε_2-KR, ε_3-UE scheme in which Alice makes one pass. Let Q be the composition of P_{KR} and P_{UE} such that Alice sends her messages in parallel, and the message of P_{KR} is used as key material in P_{UE}. Then Q is $(\varepsilon_1 + \varepsilon_2)$-KR, and it is ε_3-UE with respect to the message of P_{UE}.*

Proof: We consider the EPR version of Q. Eve creates a state that can be written as $\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}$, where the labels '1' and '2' refer to the EPR pairs intended for P_{KR} and P_{UE} respectively, and A,B refers to the EPR parts going to Alice and Bob. As in Section 4.3 we introduce different notation for the same CPTP map depending on the property that we are looking at (KR or UE). Thus we have CPTP maps $\mathcal{Q}_{1\mathrm{KR}}$, $\mathcal{Q}_{1\mathrm{UE}}$, $\mathcal{Q}_{2\mathrm{KR}}$, $\mathcal{Q}_{2\mathrm{UE}}$, with

$$(\mathcal{Q}_{2\mathrm{KR}} \circ \mathcal{Q}_{1\mathrm{KR}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \mathcal{Q}_{2\mathrm{KR}}(\rho^{M_1\tilde{K}_1T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \rho^{\tilde{K}_1T_1M_2\tilde{K}_2T_2\mathrm{E}} \tag{34}$$

$$(\mathcal{Q}_{2\mathrm{UE}}^{\mathrm{acc}} \circ \mathcal{Q}_{1\mathrm{UE}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \mathcal{Q}_{2\mathrm{UE}}^{\mathrm{acc}}(\rho^{M_1K_1\tilde{K}_1T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \rho_{[\Omega=1]}^{M_1K_1\tilde{K}_1T_1M_2K_2\tilde{K}_2T_2\mathrm{E}}. \tag{35}$$

With respect to the KR property, the ideal functionality is $\mathcal{Q}_{2\mathrm{KR}}^{\mathrm{ideal}} \circ \mathcal{Q}_{1\mathrm{KR}}^{\mathrm{ideal}}$. With respect to UE the ideal functionality is as follows. In case of `reject` there are no requirements. In case of `accept` the M_2 is protected by $\mathcal{Q}_{2\mathrm{UE}}^{\mathrm{acc,ideal}}$ even if $\mathcal{Q}_{1\mathrm{UE}}$ does not behave ideally; hence the ideal functionality is described by the mapping $\mathcal{Q}_{2\mathrm{UE}}^{\mathrm{acc,ideal}} \circ \mathcal{Q}_{1\mathrm{UE}}$. We have

$$(\mathcal{Q}_{2\mathrm{KR}}^{\mathrm{ideal}} \circ \mathcal{Q}_{1\mathrm{KR}}^{\mathrm{ideal}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \mathcal{Q}_{2\mathrm{KR}}^{\mathrm{ideal}}(\rho^{M_1\tilde{K}_1} \otimes \rho^{T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \rho^{\tilde{K}_1M_2\tilde{K}_2} \otimes \rho^{T_1T_2\mathrm{E}} \tag{36}$$

$$(\mathcal{Q}_{2\mathrm{UE}}^{\mathrm{acc,ideal}} \circ \mathcal{Q}_{1\mathrm{UE}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \mathcal{Q}_{2\mathrm{UE}}^{\mathrm{acc,ideal}}(\rho^{M_1K_1\tilde{K}_1T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}})$$
$$= \rho^{M_2} \otimes \rho_{[\Omega=1]}^{M_1K_1\tilde{K}_1T_1K_2\tilde{K}_2T_2\mathrm{E}}. \tag{37}$$

---

[8]The rate for that combination is obtained as follows. The UE step needs $n_{\mathrm{UE}} = L/[1 - 2h(\beta)]$ qubits. Then n_{UE} bits of key need to be refreshed using QKD; this takes $n_{\mathrm{QKD}} = n_{\mathrm{UE}}/[1 - 2h(\beta)]$ qubits. The rate is $L/(n_{\mathrm{UE}} + n_{\mathrm{QKD}}) = \frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$.

It is given that $\|\mathcal{Q}_{1\mathrm{KR}} - \mathcal{Q}_{1\mathrm{KR}}^{\mathrm{ideal}}\|_\diamond \le \varepsilon_1$, and $\|\mathcal{Q}_{2\mathrm{KR}} - \mathcal{Q}_{2\mathrm{KR}}^{\mathrm{ideal}}\|_\diamond \le \varepsilon_2$, and $\|\mathcal{Q}_{2\mathrm{UE}} - \mathcal{Q}_{2\mathrm{UE}}^{\mathrm{ideal}}\|_\diamond \le \varepsilon_3$. The KR property of Q follows trivially from

$$\left\| \mathcal{Q}_{2\mathrm{KR}} \circ \mathcal{Q}_{1\mathrm{KR}} - \mathcal{Q}_{2\mathrm{KR}}^{\mathrm{ideal}} \circ \mathcal{Q}_{1\mathrm{KR}}^{\mathrm{ideal}} \right\|_\diamond \le \left\| \mathcal{Q}_{1\mathrm{KR}} - \mathcal{Q}_{1\mathrm{KR}}^{\mathrm{ideal}} \right\|_\diamond + \left\| \mathcal{Q}_{2\mathrm{KR}} - \mathcal{Q}_{2\mathrm{KR}}^{\mathrm{ideal}} \right\|_\diamond \le \varepsilon_1 + \varepsilon_2. \quad (38)$$

The UE property with regard to M_2 follows from

$$\left\| \mathcal{Q}_{2\mathrm{UE}} \circ \mathcal{Q}_{1\mathrm{UE}} - \mathcal{Q}_{2\mathrm{UE}}^{\mathrm{ideal}} \circ \mathcal{Q}_{1\mathrm{UE}} \right\|_\diamond \le \left\| \mathcal{Q}_{2\mathrm{UE}} - \mathcal{Q}_{2\mathrm{UE}}^{\mathrm{ideal}} \right\|_\diamond \le \varepsilon_3. \quad (39)$$

$\square$

Remark. It is possible to send the current-round e via QKR instead of the next-round key e'. This would make e into a short-term variable instead of a long-term key, and would make it possible to elegantly use Lemma 2 in the security proof. However, it would also complicate the security analysis of the *combined* scheme. We will not pursue this possibility here.

8 Comparison to other schemes

We briefly comment on the round complexity and the asymptotic rate of the protocols proposed in this paper as compared to other schemes. The word 'round complexity' here is not to be confused with the N rounds in our protocol. For a given message chunk μ_j we count *the number of times Alice has to send something*, and refer to this number as Alice's number of *passes*. The rate is defined as the size of the message divided by the number of qubits. We compare against other information-theoretically secure schemes which also do not use up[9] key material,

- **QKD+OTP**. Key establishment using Quantum Key Distribution, followed by One Time Pad classical encryption. We consider efficient QKD with negligible waste of qubits [16] and the smallest possible number of communication rounds: only 2 passes by Alice.

- **QKR**. Qubit-wise prepare-and-measure Quantum Key Recycling as described in [14, 15]. Only a single pass by Alice is needed, since Alice and Bob already share key material.

- **QKD+[9]**. Key establishment using QKD, followed by Gottesman's Unclonable Encryption [9]. At least two passes by Alice are needed.

- **QKR+[9]**. Key establishment using QKR, followed by Gottesman's Unclonable Encryption. Only a single pass by Alice is needed when the two are performed in parallel [10].

The scheme properties are summarised in Table 1, and the rates are plotted in Fig. 2. (We only show 4-state encoding. The comparison holds qualitatively for 6-state encoding as well, but with slightly higher rates.) QKR is an improvement over QKD in terms of round complexity, while achieving the same rate. However, QKD and QKR over a noisy channel do not have the Unclonable Encryption property.
To our knowledge, the only existing scheme with an explicit proof of the UE property before our work was Gottesman's construction [9]. (And thus "QKD/QKR + [9]" was the only known way to have UE without net expenditure of key material.) Our best performing scheme is

---

[9]Our schemes use up key material, but this is amortised over N rounds. We neglect this expenditure for the purpose of the comparison.

[10]We don't give a proof for this combination as [9] uses a different proof technique. Intuitively security is the same as the combination described in Section 7.2

Protocol	Alice #passes	Asymptotic rate (4-state)	Unclonability
QKD + OTP	2	$1 - 2h(\beta)$	no
QKR [14, 15]	1	$1 - 2h(\beta)$	no
QKD + [9]	2	$\frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
QKR + [9]	1	$\frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
KRUE	1	$1 - 3h(\beta)$	yes
QKD + KRUE*	2	$\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
QKR + KRUE*	1	$\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes

Table 1: *Comparison of schemes that have no net expenditure of key material upon* `accept`.
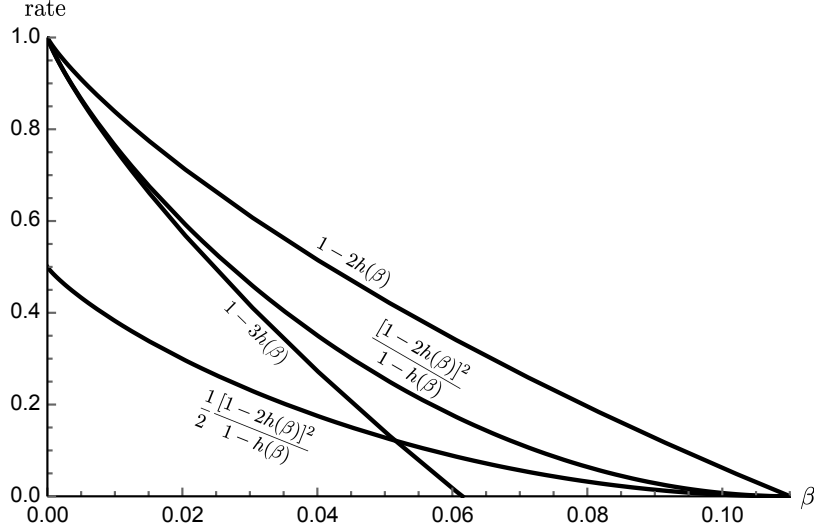

Figure 2: *Asymptotic communication rates (4-state) as a function of the noise parameter β.*

QKR+`KRUE`*, with one pass from Alice and double the rate of QKR + [9]. Our sub-optimal scheme `KRUE` has a better rate than QKD/QKR + [9] at noise levels below $\beta \approx 0.052$.

The above comparison does not contain the KR schemes [7, 12], because [7] is defined only for the noiseless case $\beta = 0$, while [12] has low rate ($\leq \frac{1}{3}$) and limited noise tolerance. Note that [7] has the UE property by Lemma 2, and we suspect that [12] satisfies a version of unclonability with a somewhat modified definition that allows for a reduction of the min-entropy of some of the keys. We believe that the QKR scheme [15] can be tweaked to have the UE property by doing more privacy amplification; this would probably lead to the same rate as `KRUE`.

We briefly comment on the key sizes. The key material used in `KRUE` consists of the OTP $z \in \{0,1\}^\ell$, the hash seed $u \in \{0,1\}^k$, the basis choice $B \in \mathcal{B}^n$, the redundancy mask $e \in \{0,1\}^{n-k}$, the authentication keys $k_{\mathrm{MAC}} \in \{0,1\}^\lambda$, $k_{\mathrm{fb}} \in \{0,1\}^\lambda$ and the OTP $k_{\mathrm{OTP}} \in \{0,1\}$. Counting only contributions proportional to n, the total size in bits is $\ell + n + n \log \mathcal{B} + \mathcal{O}(1)$. With $\ell \approx L + nh(\beta)$ and $n \approx L/[1-3h(\beta)]$ we can write the total size as $L\frac{2 + \log|\mathcal{B}| - 2h(\beta)}{1 - 3h(\beta)} + \mathcal{O}(1)$. The keys are expended over a block of N rounds (or $\leq N$ in case of `reject`). If there are no `reject`s, the 'amortised' key expenditure per round equals the above key size divided by N, which can be made much smaller than L.

The key size of QKR+`KRUE`* has a slightly different dependence on the noise parameter β.

17

For the 4-state case, sending an L-bit message via KRUE* requires $L + 2n + \mathcal{O}(1)$ bits of key, with $n \approx L/[1 - 2h(\beta)]$. Sending $nh(\beta)$ bits via the QKR scheme [14] takes a further $4\frac{nh(\beta)}{1-2h(\beta)}$ bits. This adds up to $L[1 + \frac{2}{[1-2h(\beta)]^2}] + \mathcal{O}(1)$ bits.

Gottesman's scheme has somewhat shorter keys, total length $L\frac{2-h(\beta)}{1-2h(\beta)} + \mathcal{O}(1)$, but it needs to refresh $\approx L/[1 - 2h(\beta)]$ bits every round.

9 Discussion

We have proven, in the proof framework developed by Renner et al., that quantum encryption can have Unclonability (as defined by Gottesman) as well as Key Recycling in the case of noisy channels. We achieve low communication complexity: there is no need for classical communication from Alice to Bob. The communication rate of KRUE is $1 - 3h(\beta)$ for 4-state encoding and can be increased to $\frac{[1-2h(\beta)]^2}{1-h(\beta)}$ when combining our scheme with QKD or QKR. Our scheme works by starting from QKR and making the privacy amplification a step in the computation of the qubit payload. Gottesman's construction [9] does something very similar, and hence one might try to construct a variant of our UE-KR protocol that is closer to [9]. This would have the advantage that there is no longer a seed u that needs to be stored as part of the keys, as [9] employs ECC-based privacy amplification. However, the proof technique that we use, with its reliance on hash families, does not work for ECC-based privacy amplification.

Our best performing scheme, QKR+KRUE*, has a lower rate than QKD/QKR. (But interestingly the rate is positive on the same β-interval.) It is an open question whether the rate decrease of UE schemes with respect to QKD is unavoidable. The error-correction redundancy data has to be somehow protected; this requirement does not exist in QKD. Yet, the UE requirement makes it difficult to protect the redundancy, as long-term keys will leak eventually. Perhaps an error-correcting scheme like [11], which was used in [12], can help here.

Our protocols (temporarily) hide the accept/reject feedback bit ω. This is a technicality that allows us to re-use b in un-altered form. The alternative would be to send ω in the clear and then either (i) partially refresh b as in [15], or (ii) find a way to cope with a reduced entropy of b as in [12]. Note that it is not realistic to hide a *large* accumulation of ω-feedbacks from Eve. Alice and Bob would have to act for a long time in a way that, to an external observer, does not depend on the ωs. However, Eve may be able to observe e.g. how often Alice and Bob have to engage in QKD to refill their key 'reservoir', which reveals the total number of rejects. For a *small* accumulation (e.g. size N) we expect that it *is* realistic to hide the feedbacks temporarily.

The downside associated with encoding a message directly into qubits is the vulnerability to erasures (particle loss) on the quantum channel. Whereas QKD can just ignore erasures, in QKR they have to be compensated by the error-correcting code, which incurs a serious rate penalty.

Acknowledgements

A   QKD asymptotics

We consider a QKD version that looks as much as possible like our protocol, and apply Renner's proof technique to quickly derive bounds on the diamond norm. For brevity we ignore message authentication tags and their failure probability, since they do not affect the asymptotics. We do not consider two-way postprocessing tricks like advantage distillation. We refer to the resulting rates in this Appendix as the asymptotic rate of QKD-with-one-way-postprocessing.

QKD Protocol.

Eve sends EPR pairs, in the singlet state. Alice and Bob randomly choose measurement bases from the set $\mathcal{B}$, perform their measurements, and then publicly announce their basis choices. They disregard all events where they chose different bases, and are left with n bits. Alice has measurement outcome $s \in \{0,1\}^n$, Bob has $t \in \{0,1\}^n$. Alice generates random $x \in \{0,1\}^n$, $u \in \{0,1\}^n$. She computes a mask $a = s \oplus x$ and OTP $z = \Phi_u(x)$. She sends a to Bob over an authenticated channel. She also sends the syndrome $\sigma = \mathtt{Syn}(x) \in \{0,1\}^{n-k}$, either in the clear or OTP'ed. (We will analyze both options.)

Bob computes $x' = t \oplus \bar{a}$ and tries to reconstruct x from x' and σ. If he finds a $\hat{x}$ satisfying $|\hat{x} \oplus x'| \leq n\beta$ he sets $\omega = 1$, otherwise $\omega = 0$. He sends ω to Alice.

In case $\omega = 0$ Alice sets $c = \perp$. In case $\omega = 1$ she sets $c = m \oplus z$. Alice sends c, u. If $\omega = 1$ Bob reconstructs $\hat{z} = \Phi_u(\hat{x})$ and $\hat{m} = c \oplus \hat{z}$.

Analysis in case of OTP'ed syndrome.

Eve observes b, u, a, c, ω and holds a quantum state ρ^{E}_{bst} correlated to b, s, t. The message m must be secure given Eve's information. The output state of the QKD protocol is given by

$$\mathcal{E}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle mbuac\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\mathrm{E}}_{bst} \delta_{\omega,\theta_{st}} [\omega \delta_{c,m\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \quad (40)$$

The idealized output state is obtained as $\mathbb{E}_m |m\rangle\langle m| \otimes \mathrm{tr}_M \mathcal{E}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}})$, which yields

$$\mathcal{F}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle mbuac\omega| \otimes \mathop{\mathbb{E}}_{st} \rho^{\mathrm{E}}_{bst} \delta_{\omega,\theta_{st}} [\omega \mathop{\mathbb{E}}_{m'} \delta_{c,m'\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \quad (41)$$

The difference is given by

$$
\begin{aligned}
(\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}})(\rho^{\mathrm{ABE}}) &= \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac} |mbuac, \omega = 1\rangle\langle mbuac, \omega = 1| \\
&\otimes \mathop{\mathbb{E}}_{st} \rho^{\mathrm{E}}_{bst} \theta_{st} [\delta_{c,m\oplus\Phi_u(a\oplus s)} - \mathop{\mathbb{E}}_{m'} \delta_{c,m'\oplus\Phi_u(a\oplus s)}].
\end{aligned}
\quad (42)
$$

This expression can be seen as the difference between two sub-normalized states which both have norm P_{corr}. Hence an upper bound $\|\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}}\|_\diamond \leq P_{\mathrm{corr}}$ immediately follows. Furthermore, from (42) it follows that

$$\|\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}}\|_\diamond \leq \frac{1}{2} \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{ac} \left\| \mathop{\mathbb{E}}_{st} \rho^{\mathrm{E}}_{bst} \theta_{st} 2^{\ell} [\delta_{c,m\oplus\Phi_u(a\oplus s)} - \mathop{\mathbb{E}}_{m'} \delta_{c,m'\oplus\Phi_u(a\oplus s)}] \right\|_1. \quad (43)$$

Expanding the trace norm as $\|A\|_1 = \mathrm{tr} \sqrt{A^\dagger A}$ we write the right hand side as

$$\frac{1}{2} \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{ac} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (44)$$

$$\mathrm{tr} \sqrt{ \mathop{\mathbb{E}}_{ss't t'} \theta_{st}\theta_{s't'} \rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{bs't'} 2^{2\ell} [\delta_{\Phi_u(a\oplus s),m\oplus c} - \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(a\oplus s),m'\oplus c}][\delta_{\Phi_u(a\oplus s'),m\oplus c} - \mathop{\mathbb{E}}_{m''} \delta_{\Phi_u(a\oplus s'),m''\oplus c}]}.$$

19

Using Jensen's inequality for operators we 'pull' $\mathbb{E}_u$ and $\mathbb{E}_m$ under the square root and then make use of the pairwise-independent properties of Φ_u when acted upon with $\mathbb{E}_u$. This yields

$$2^{2\ell} \mathbb{E}_{mu} [\delta_{\Phi_u(a\oplus s),m\oplus c} - \mathbb{E}_{m'} \delta_{\Phi_u(a\oplus s),m'\oplus c}][\delta_{\Phi_u(a\oplus s'),m\oplus c} - \mathbb{E}_{m''} \delta_{\Phi_u(a\oplus s'),m''\oplus c}] = 2^\ell \delta_{ss'}(1 - \mathbb{E}_{mm'} \delta_{mm'})$$
$$< 2^\ell \delta_{ss'} \quad (45)$$

which leads to

$$\|\mathcal{E}_{\text{QKD}} - \mathcal{F}_{\text{QKD}}\|_\diamond < \tfrac{1}{2} \mathbb{E}_b \,\text{tr} \sqrt{2^\ell \mathbb{E}_{ss'tt'} \theta_{st}\theta_{s't'} \rho_{bst}^{\text{E}}\rho_{bs't'}^{\text{E}} \delta_{ss'}}. \quad (46)$$

Next we use $\theta_{st} \leq 1$ and $\mathbb{E}_t \rho_{bst}^{\text{E}} = \rho_{bs}^{\text{E}}$, yielding $\|\mathcal{E}_{\text{QKD}} - \mathcal{F}_{\text{QKD}}\|_\diamond < \tfrac{1}{2} \mathbb{E}_b \,\text{tr} \sqrt{2^\ell \mathbb{E}_{ss'} \rho_{bs}^{\text{E}}\rho_{bs'}^{\text{E}} \delta_{ss'}}$. Combining the two obtained bounds gives

$$\|\mathcal{E}_{\text{QKD}} - \mathcal{F}_{\text{QKD}}\|_\diamond \leq \min\left(P_{\text{corr}}, \tfrac{1}{2} \mathbb{E}_b \,\text{tr} \sqrt{2^\ell \mathbb{E}_{ss'} \rho_{bs}^{\text{E}}\rho_{bs'}^{\text{E}} \delta_{ss'}}\right). \quad (47)$$

Using Post-selection, random Paulis and smooth Rényi entropy techniques, it has been shown [15, 19] that the right hand side of (47) can be upper bounded as $\propto \sqrt{2^{\ell-n+nh(\beta)}}$ for BB84 bases, and as $\propto \sqrt{2^{\ell-n-nh(\beta)+nh(1-\frac{3}{2}\beta,\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})}}$ for 6-state QKD.

When n is increased then either P_{corr} becomes exponentially small (if Eve's noise γ exceeds β) or (when $\gamma \leq \beta$) the expression under the square root becomes exponentially small, provided ℓ is set smaller than some threshold value ℓ_{max}. This threshold is given by $\ell_{\text{max}}^{\text{BB84}} = n - nh(\beta)$ and $\ell_{\text{max}}^{\text{6state}} = n + nh(\beta) - nh(1 - \frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$. Taking into account the key expenditure for masking the syndrome $\text{Syn}(x)$, the asymptotic rate is $r = \ell_{\text{max}}/n - h(\beta)$, i.e. $r^{\text{BB84}} = 1 - 2h(\beta)$; $r^{\text{6state}} = 1 - h(1 - \frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$.

Analysis in case of plaintext syndrome

We indicate the differences w.r.t. the analysis above. Eq. (40) gains an extra part due to the syndrome σ and becomes

$$\mathcal{E}_{\text{QKD}}^{\text{plain}}(\rho^{\text{ABE}}) = \mathbb{E}_{mbu} 2^{-n} \sum_{ac\sigma\omega} |mbuac\sigma\omega\rangle\langle mbuac\sigma\omega| \otimes \mathbb{E}_{st} \rho_{bst}^{\text{E}} \delta_{\omega,\theta_{st}} \delta_{\sigma,\text{Syn}(a\oplus s)}[\omega\delta_{c,m\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}].$$
$$(48)$$

The factor $\delta_{\sigma,\text{Syn}(a\oplus s)}$ is carried along untouched in the whole computation up to (44), where it gets doubled to $\delta_{\sigma,\text{Syn}(a\oplus s)}\delta_{\sigma,\text{Syn}(a\oplus s')}$. However, the $\delta_{ss'}$ produced in (45) undoes the doubling. One extra step is needed. The sum $\sum_e$ is rewritten as $2^{n-k} \cdot \frac{1}{2^{n-k}} \sum_\sigma$, and Jensen's inequality is used, 'pulling' the averaging operation $\frac{1}{2^{n-k}} \sum_\sigma$ into the square root, where it acts on $\delta_{\sigma,\text{Syn}(a\oplus s)}$, giving rise to a constant 2^{k-n}.

$$\|\mathcal{E}_{\text{QKD}}^{\text{plain}} - \mathcal{F}_{\text{QKD}}^{\text{plain}}\|_\diamond \leq \min\left(P_{\text{corr}}, \tfrac{1}{2} \mathbb{E}_b \,\text{tr} \sqrt{2^\ell 2^{n-k} \mathbb{E}_{ss'} \rho_{bs}^{\text{E}}\rho_{bs'}^{\text{E}} \delta_{ss'}}\right). \quad (49)$$

The ℓ_{max} is decreased by an amount $n - k$, but the rate is exactly the same as before, since this time there is no key expenditure of $n - k$ bits for encrypting the syndrome.

References

[1] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (1991), 661 –663.

[2] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, and J. Oppenheim, *The universal composable security of quantum key distribution*, Theory of cryptography, 2005, pp. 386–406.

[3] A. Broadbent and S. Lord, *Uncloneable quantum encryption via random oracles* (2019). https://eprint.iacr.org/2019/257.

[4] C.H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, IEEE International Conference on Computers, Systems and Signal Processing (1984), 175–179.

[5] C.H. Bennett, G. Brassard, and S. Breidbart, *Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP*, Natural Computing **13** (2014), 453–458. Original manuscript 1982.

[6] M. Christandl, R. König, and R. Renner, *Postselection technique for quantum channels with applications to quantum cryptography*, Phys. Rev. Lett. **102** (2009Jan), 020504.

[7] I.B. Damgård, T.B. Pedersen, and L. Salvail, *A Quantum Cipher with Near Optimal Key-Recycling*, CRYPTO (2005).

[8] D. Bruß, *Optimal eavesdropping in quantum cryptography with six states*, Phys. Rev. Lett. **81** (1998), no. 14, 3018–3021.

[9] D. Gottesman, *Uncloneable encryption*, Quantum Information and Computation **3** (2003), no. 6, 581–602.

[10] D. Gottesman and J. Preskill, *Secure quantum key distribution using squeezed states*, Phys. Rev. A **63** (2001), 022309.

[11] Y. Dodis and A. Smith, *Correcting errors without leaking partial information*, ACM STOC, 2005, pp. 654–663.

[12] S. Fehr and L. Salvail, *Quantum authentication and encryption with key recycling*, Eurocrypt, 2017, pp. 311–338.

[13] B. Kraus, N. Gisin, and R. Renner, *Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication*, Phys.Rev.Lett. **95** (2005), 080501.

[14] D. Leermakers and B. Škorić, *Quantum Alice and Silent Bob: Qubit-based Quantum Key Recycling with almost no classical communication*. https://eprint.iacr.org/2019/875.

[15] _____, *Security proof for Quantum Key Recycling with noise*, Quantum Information Processing **19** (2019).

[16] H.-K. Lo, H.F. Chau, and M. Ardehali, *Efficient Quantum Key Distribution scheme and proof of its unconditional security*, Journal of Cryptology **18** (2005), 133–165.

[17] R. T. Moenck, *Fast Computation of GCDs*, Proceedings of the fifth annual ACM Symposium on Theory of Computing, 1973, pp. 142–151.

[18] C. Portmann, *Quantum authentication with key recycling*, Advances in Cryptology – Eurocrypt 2017, 2017, pp. 339–368.

[19] R. Renner, *Security of quantum key distribution*, Ph.D. Thesis, 2005.

[20] P. Shor and J. Preskill, *Simple proof of security of the BB84 quantum key distribution protocol*, Phys.Rev.Lett. **85** (2000), 441.

[21] M. Tomamichel and A. Leverrier, *A largely self-contained and complete security proof for quantum key distribution*, Quantum **1** (201707), 14.

[22] T. Sasaki, Y. Yamamoto, and M. Koashi, *Practical quantum key distribution protocol without monitoring signal disturbance*, Nature **509** (2014), 475–478.

[23] B. Škorić and M. de Vries, *Quantum Key Recycling with eight-state encoding. (The Quantum One Time Pad is more interesting than we thought)*, International Journal of Quantum Information (2017).

[24] M.N. Wegman and J.W. Carter, *New hash functions and their use in authentication and set equality*, Journal of computer and system sciences **22** (1981), 265–279.

[25] W.K. Wootters and W.H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.